

집적영상에서의 혼돈 수열을 사용한 3D 물체의 암호화

이소위* · 조성진** · 김석태***

3D Object Encryption Employed Chaotic Sequence in Integral Imaging

Xiao-Wei Li* · Sung-Jin Cho** · Seok-Tae Kim***

요 약

본 논문에서는 집적영상에서 가상광학과 혼돈 수열(chaos sequence)을 결합하여 3차원 물체 영상을 암호화하는 새로운 방법을 제안한다. 먼저 가상 핀홀 배열(virtual pinhole array)을 통하여 2차원 요소영상 배열(EIA)을 생성한 후, 이를 이용해 3차원 물체를 디지털로 만든다. 그 후 혼돈 수열의 논리적 연산을 통해 최종 암호화 영상을 만든다. 이러한 방법은 영상 데이터를 시각화하기 위한 영상의 기본 정보인 픽셀의 값을 변환시키기 때문에 기존의 암호화 방법보다 향상된 암호화 결과를 얻을 수 있다. 실험을 통해 본 암호화 방법의 유효성과 안정성을 검증한다.

ABSTRACT

This paper presents a novel three-dimensional (3D) object encryption scheme by combining the use of the virtual optics and the chaotic sequence. A virtual 3D object is digitally produced using a two-dimensional (2D) elemental image array (EIA) created with a virtual pinhole array. Then, through a logistic mapping of chaotic sequence, a final encrypted video can be produced. Such method converts the value of a pixel which is the basic information of an image. Therefore, it gives an improved encryption result compared to other existing methods. Through computational experiments, we were able to verify our method's feasibility and effectiveness.

키워드

Virtual Optics, 3D Object, Pinhole Array, Encryption
가상 광학, 3D 물체, 핀홀 어레이, 암호화

1. INTRODUCTION

In today's world of developing technology, it is becoming more difficult to keep information safe. Information security technique has become indispensable. Optical security techniques with digital transmission have attracted more attention

due to the convenience in transmitting enormous data through the network[1-5]. Refregier and Javidi[6] proposed a double random phase encoding method that encodes an input image into stationary white noise. Unnikrishnan et al.[7] presented a fractional Fourier transform[8-9] based on image encoding method that set the second random mask

* Sichuan University, (xwli2hang@gmail.com)

** 부경대학교 응용수학과(sjcho@pknu.ac.kr)

*** 교신저자 : 부경대학교 정보통신공학과

• 접수일 : 2018. 01. 06

• 수정완료일 : 2018. 02. 24

• 게재확정일 : 2018. 04. 15

• Received : Jan. 06, 2018, Revised : Feb. 24, 2018, Accepted : Apr. 15, 2018

• Corresponding Author : Seok Tae Kim

Dept. of Information & Communications Engineering,
Pukyong National University.

Email : setakim@pknu.ac.kr

on the fractional plane rather than the Fourier plane. Situand Zhang[10] employed a lensless encoding system based on double phase encoding in the Fresnel domain[11]. This encoding system provides higher security due to the positions of the two phase masks. The two phase masks, as well as operation wave length, are used as the decryption keys. Afterwards, many encryption methods based on digital holography[12], multiplexing[13], gyrator transform[14–17], etc. have been proposed.

One of the primary objectives for encryption methods is to protect information from unauthorized users. Optical encryption has attracted wide attention due to its high speed, parallel processing and large capacity storage of image encryption technology. Because of the intrinsic parallelism and high processing speed, optical information processing system is still considered to be a perspective candidate over the past decade. Some are done by Fourier transform, Fresnel transform, or fractional Fourier transforms which all concentrate on encoding information using the DRPE(: Double Random Phase Encoding).

In DRPE, an input image is encoded into a stationary white noise. The cipher text is generated by using two statistically independent random phases which locate in a 4-f system at the input and Fourier planes, respectively. The major advantage of DRPE is that it can provide high security and easily implement with a 4-f optical architecture. To reconstruct the encrypted image, there are two main approaches. First approach decrypts the encoded image using DRPE method. For such method, the original image is a necessity. On the other hand, the second approach directly recovers the encrypted image using DRPE method without the original host image. There are both advantages and disadvantages in the two methods. The former one can provide high quality, however, it requires a complicated computation in the

iterative process because a lot of operations and transformations are unavoidable. Moreover, it is a burdensome process to store and transmit the original image. Even though the latter method does not need to transmit and store the original image, the reconstructed image quality is degraded because of the added noise from the original image in the process.

However, the implementation of an optical system provokes various practical issues such as a shortfall of actual optical equipment, a demand for manufacturing RPMs(: Random Phase Masks), and a difficulty of their alignment in the decryption process. Furthermore, in this paper, to perform encryption of the original image with a random noise distribution, a phase conjugation operation was carried out. However, the decrypted image ended up with a low resolution and illustrated the difficulty of removing the random noise in the decryption process. Likewise, there is a possibility of imposing a heavy burden on the practical encryption system when a large amount of hologram data processing is required.

Generally, 3D integral imaging is one of the most valuable techniques for 3D object encryption, because it can provide high robustness. Even though there are such advantages in this method, it has a thorny problem: limited image resolution. The image is optically recorded and reconstructed; yet, it's still plagued by a number of issues. For instance, diffractions and physical limitations of the optical devices are likely to provide reconstructed images with low-resolution and to result in degraded image quality. In order to solve this problem, Hong et al.[18] proposed a CIIR(: Computational Integral Imaging Reconstructed) [19–24] technique. However, in the pickup process of Hong et al. method, the EIA(: Elemental Image Array) was recorded through a lenslet array onto the pickup plane. Due to scattering light, the reconstructed image of the optically-generated EIA

with low resolution diffracted ray and still exhibited some physical limitations of the optical devices.

To alleviate these practical problems discussed above, an encryption scheme using computer-generated integral imaging and logistic mapping of chaotic sequence is studied. Computer can be generated integral imaging that picks-up and displays image by using a computer. The central key to the proposed design is the elemental image generation and reconstruction by a computer. The above problems will be readily solved. This is because computer-generated integral imaging technique has no diffraction and device limitations.

II. THEORETICAL ANALYSIS

2.1 Computer-generated integral imaging

The computer-generated integral imaging technique as a novel technique can overcome or mitigate above-mentioned problems. The overall concept of optical image processing based on CGII (Computer-Generated Integral Imaging) is depicted in Fig. 1 CGII is used, in which an optical image can be computationally recorded in the form of 2D EIA through a virtual pinhole array. The image can be digitally reconstructed by inversely mapping each elemental image through a virtual pinhole array. Using CGII, image quality is improved compared to the image using optical method. The reason is that CGII brings no diffraction and no device limitations. The proposed optical image encryption method can be achieved by the computer simulation.

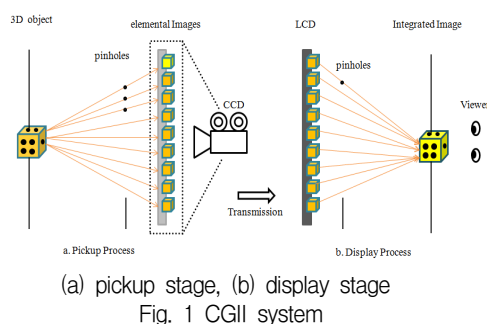


Fig. 1 illustrates the operational principle of the CGII technique for the object image picking up and reconstructing. The pickup process of CGII is displayed in Fig. 1(a). The object image locates at the distance of $z = l$ and the EIA plane locates at the distance of $z = g$. Each elemental image is recorded through a process of pickup and is projected inversely through each pinhole. Meanwhile, as shown in Fig. 1(b), the reconstructed process is based on ray optics pinhole imaging theory. All elemental images are inversely magnified through the virtual pinhole array and summed together at the reconstructed image output plane of $z = l$. By computer simulation system, each of elemental images can be inversely reduced according to the magnification factor of $a = g/l$ ($g < l$). However, in the reconstructed process, the EIA is inversely magnified based on the magnification factor of $\beta = g/l$, in which l is the distance between the virtual pinhole array and the object image plane and g is the distance between the virtual pinhole array and the EIA plane.

2.2 Chaotic sequence

Chaotic sequence is a kind of pseudorandom, which is produced by a nonlinear equation. The equation for logistic mapping chaos is given by:

$$x(n+1) = \rho x(n)(1-x(n)) \quad (1)$$

where $0 < x(n+1) < 1$, and $n = 0, 1, 2, \dots$, and $0 \leq \rho \leq 4$. When $3.5699 \dots \leq \rho \leq 4$, the sequence is in the chaotic state. All the sequences are very sensitive to the initial values.

III. EXPERIMENTAL RESULTS

In order to exhibit the efficiency of the proposed method, we presented different computational experiments for 3D image encryption. The experimental structure is explained in Fig. 2.

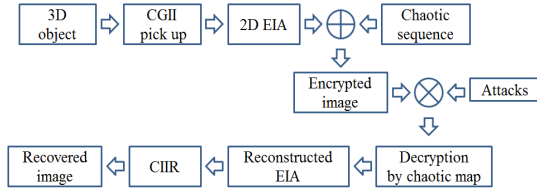


Fig. 2 Block diagram of the proposed image encryption scheme

In CGII, the lenslet array was replaced by the virtual pinhole array for experiments. First, we obtain the EIA by using CGII system. The elemental images of the target object are synthesized through a virtual pinhole array of CGII system. In this experiment, we used a 3D virtual object, composed of image patterns. Image “dice” and “elephant” are shown in Fig. 3. Both character patterns have 900×900 pixels. These two patterns were longitudinally located at the distance of $l = 18\text{mm}$ and $l = 36\text{mm}$, respectively. The virtual pinhole array consists of 30×30 pinholes, placed at $z = 0\text{mm}$. The pitch of each pinhole is 1.08mm and the distance ‘ g ’ between the display panel and the VPA is 3mm . The computer-generated EIA is synthesized by the ray tracing theory. The results are shown in Fig. 3.

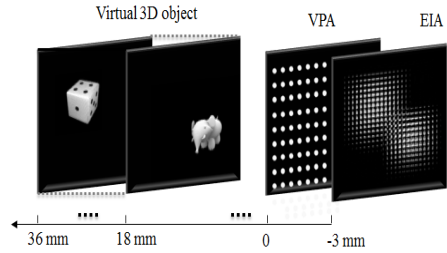


Fig. 3 Converted 3D object to 2D EIA

In the next step, the produced EIA is scrambled by the chaotic map with the input initial parameters $x(0) = 0.23$ and $\rho = 3.56993012$. The obtained encrypted image is shown in Fig. 4(b).

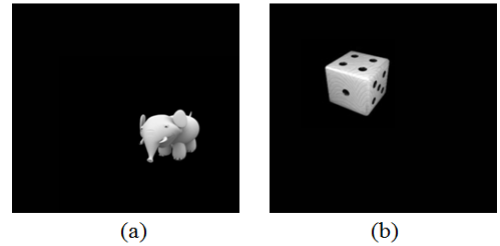


Fig. 4 Converted 3D object to 2D EIA

Fig. 4 shows the original plane images ‘elephant’ and ‘dice’.

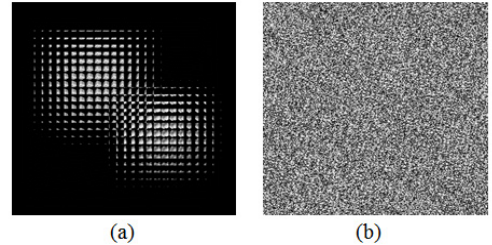


Fig. 5 Recorded 2D EIA (a) and encrypted image (b)

The 3D plane images were digitally reconstructed from the retrieved EIA using CIIR. The 3D reconstructed plane images located at the distance of $z = 18$ and 36mm are displayed in Fig. 5.

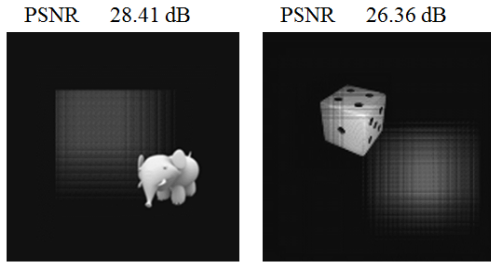


Fig. 6 Reconstructed 3D plane images by the proposed method

In order to assess the improved quality of the reconstructed images, we introduce PSNR(Peak Signal-to-Noise Ratio). The calculated values are displayed in Fig. 6.

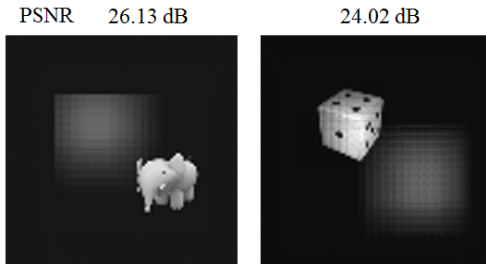


Fig. 7 Reconstructed images based on Hong et al. method

To further demonstrate our model, we compare two different methods and analyze the qualities of the recovered images. By comparing our method to the proposed methods of Hong et al, we were able to conclude that our model reconstructs the object planes more precisely. We explicitly depict the 3D plane images using methods proposed by Hong et al in Fig. 7.

For our method, the PSNR of the two plane images of “elephant” and “dice” were 28.41dB and 26.36dB, respectively. Compared with Hong’s method, the PSNRs are improved 2.05dB and 2.11dB, that is, the image quality of this scheme has been improved 7.85% and 8.78%.

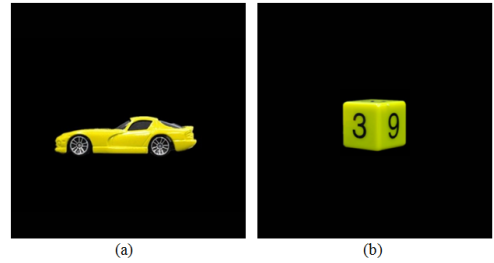


Fig. 8 Recorded 2D EIA (a) and encrypted image (b)

Fig. 8 shows the original color plane images ‘car’ and ‘dice’ with the size of 900×900 .

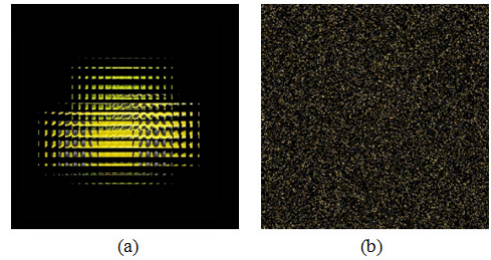


Fig. 9 Recorded 2D EIA (a) and encrypted image (b)

Fig. 9 shows picked up EIA and encrypted images. From the simulation results, we can see that the encryption result is good.

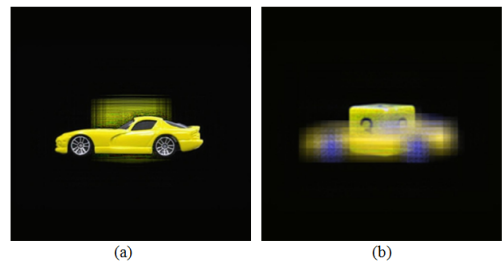


Fig. 10 Recorded 2D EIA (a) and encrypted image (b)

Fig. 10 shows the reconstructed plane images where the car and dice located in the same horizontal direction at the distance of 18mm and 36mm, respectively.



Fig. 11 Reconstructed plane images with Gaussian noise attack (a) and (b)

Fig. 11 shows the reconstructed car and dice plane images from the encrypted images with Gaussian noise attack. Fig. 11(a) displays the reconstructed plane images 'car' with variance of 0.01, 0.05 and 0.1. Fig. 11(b) shows the reconstructed plane images 'dice' with variance of 0.01, 0.05 and 0.1.

IV. CONCLUSION

In this paper, a 3D object encryption method using chaotic map and computer generated integral imaging technique is proposed. In the encryption process, an image is initially picked up by the CGII algorithm, and then the recorded 2D elemental image array is encrypted by combined use of the chaotic sequence. The decryption operation is the reverse process of encryption.

As a result, the quality of the image is improved

using CGII compared to the one using optical method. Also, the proposed scheme provides a high security like the hologram property due to the high key space.

To demonstrate the effectiveness of the proposed method, different experiments are carried out. The simulations' results confirm the feasibility of the proposed method in practical applications. Thus, this makes a reasonably good candidate for encryption.

In addition, the CGII algorithm used in multiple ownership copyright protection provides many benefits. However, this method exists noise interference in the watermark reconstruction process. To solve such problem, we will continue to study and develop an effective noise-removed approach.

Acknowledgment

This work was supported by a Research Grant of Pukyong National University (2016 year).

References

- [1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 20, no. 7, 1995, pp. 767-769.
- [2] X. Li, S. Cho, and S. Kim, "A 3D image encryption technique using computer-generated integral imaging and cellular automata transform," *Optik - Int. J. for Light and Electron Optics*, vol. 125, no. 13, July 2014, pp. 2983-2990.
- [3] K. Kim, D. Wang, and S. Han, "Home Security System Based on IoT," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 12, no. 1, 2017, pp. 147-154.
- [4] D. Kim, "Implementation Plan and Requirements Analysis of Access Control for Cyber Security of Nuclear Power Plants," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 1,

- 2016, pp. 1-8.
- [5] H. Kim, S. Cho, U. Choi, M. Kwon and G. Kong, "Synthesis of Uniform CA and 90/150 Hybrid CA," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 3, 2016, pp. 293-302.
- [6] S. Kishk and B. Javidi, "Information hiding technique with double phase encoding," *Applied Optics*, vol. 41, no. 26, 2002, pp. 5462-5470.
- [7] J. Sang, H. Xiang, L. Fu, and N. Sang, "Security analysis and improvement on a double-random phase-encoding technique based information hiding method," *Optics Communications*, vol. 282, no. 12, June 2009, pp. 2307-2317.
- [8] S. Liu, and J. T. Sheridan, "Optical encryption by combining image scrambling techniques in fractional Fourier domains," *Optics Communications*, vol. 287, no. 1, Jan. 2013, pp. 73-80.
- [9] G. Unnikrishnan, J. Joseph, and K. Singh. "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Optics Letters*, vol. 25, no. 12, 2000, pp. 887-889.
- [10] S. Yuan, X. Zhou, and M. Alam, "Information hiding based on double random-phase encoding and public-key cryptography," *Optics Express*, vol. 17, no. 5, 2009, pp. 3270-3284.
- [11] W. Li and I. Lee, "Modified computational integral imaging-based double image encryption using fractional Fourier transform," *Optics and Lasers in Engineering*, vol. 66, no. 3, Mar. 2015, pp. 112-121.
- [12] W. Li and S. Kim, "Optical 3D watermark based digital image watermarking for telemedicine," *Optics and Lasers in Engineering*, vol. 51, no. 12, Dec. 2013, pp. 1310-1320.
- [13] Z. Liu, J. Dai, X. Sun, and S. Liu, "Color image encryption by using the rotation of color vector in Hartley transform domains," *Optics and Lasers in Engineering*, vol. 48, no. 8, 2010, pp. 800-805.
- [14] M. Abuturab, "Security enhancement of color image cryptosystem by optical interference principle and spiral phase encoding," *Applied Optics*, vol. 52, no. 8, 2013, pp. 1555-1563.
- [15] Z. Liu, M. Gong, Y. Dou, F. Liu, S. Lin, M. A. Ahmad, J. Dai, and S. Liu, "Double image encryption by using Arnold transform and discrete fractional angular transform," *Optics and Lasers in Engineering*, vol. 50, no. 2, Feb. 2012, pp. 248-255.
- [16] B. Javidi, A. Sergent, G. Zhang, and L. Guibert, "Fault tolerance properties of a double phase encoding encryption technique," *Optical Engineering*, vol. 36, no. 4, Apr. 1997. pp. 992-999.
- [17] J. Hyun, D. Hwang, D. Shin, and E. Kim, "Curved computational integral imaging reconstruction technique for resolution-enhanced display of three-dimensional object images," *Applied Optics*, vol. 46, no. 31, 2007, pp. 7697-7708.
- [18] S. Hong, J. Jang, and B. Javidi, "Three-dimensional volumetric object reconstruction using computational integral imaging," *Optics Express*, vol. 12, no. 3, 2004, pp. 483-491.
- [19] Y. Frauel and B. Javidi. "Digital three-dimensional image correlation by use of computer-reconstructed integral imaging," *Applied Optics*, vol. 41, no. 26, 2002, pp. 5488-5496.
- [20] H. Arimoto and B. Javidi, "Integral three-dimensional imaging with digital reconstruction," *Optics Letters*, vol. 26, no. 3, 2001, pp. 157-159.
- [21] D. Shin, C. Tan, B. Lee, J. Lee, and E. Kim, "Resolution-enhanced three-dimensional image reconstruction by use of smart pixel mapping in computational integral imaging," *Applied Optics*, vol. 47, no. 35, 2008, pp. 6656-6665.
- [22] D. Shin, B. Lee, and J. Lee, "Occlusion removal method of partially occluded 3D object using sub-image block matching in computational

integral imaging," *Optics Express*, vol. 16, no. 21, 2008, pp. 16294-16304.

- [23] M. Cho and B. Javidi, "Computational reconstruction of three-dimensional integral imaging by rearrangement of elemental image pixels," *J. of Display Technology*, vol. 5, no. 2, 2009, pp. 61-65.
- [24] Y. Piao and E. Kim, "Resolution-enhanced reconstruction of far 3-D objects by using a direct pixel mapping method in computational curving-effective integral imaging," *Applied Optics*, vol. 48, no. 34, 2009, pp. H222-H230.



김석태 (Seok-Tae Kim)

1983년 광운대학교 전자공학과졸업 (공학사)

1988년 Kyoto Institute of Technology, 전자공학과졸업(공학석사)

1991년 오사카대학교 통신공학과졸업(공학박사)

1999년 Univ. of washington, USA, 방문교수

2006년 Simon Fraser Univ., Canada, 방문교수

1991년~현재 부경대학교 정보통신공학과 교수

※ 관심분야 : 영상처리, 영상 암호화, Cellular automata.

저자 소개



이소위(Xiao Wei Li)

2009년 Dalian Ocean University 졸업, 중국(공학사)

2011년 부경대학교 대학원 정보통신공과 졸업(공학석사)

2014년 부경대학교 대학원 정보통신공학과 졸업(공학박사)

2017년 ~ 현재 Sichuan University 조교수, 중국

※ 관심분야 : 영상처리, 셀룰라 오토마타론, 정보보호



조성진 (Sung-Jin Cho)

1979년 강원대학교 수학교육과 졸업 (이학사)

1981년 고려대학교 대학원 수학과 졸업(이학석사)

1988년 고려대학교 대학원 수학과 졸업(이학박사)

1988년 ~ 현재 부경대학교 응용수학과 교수

※ 관심분야 : 셀룰라 오토마타론, 정보보호